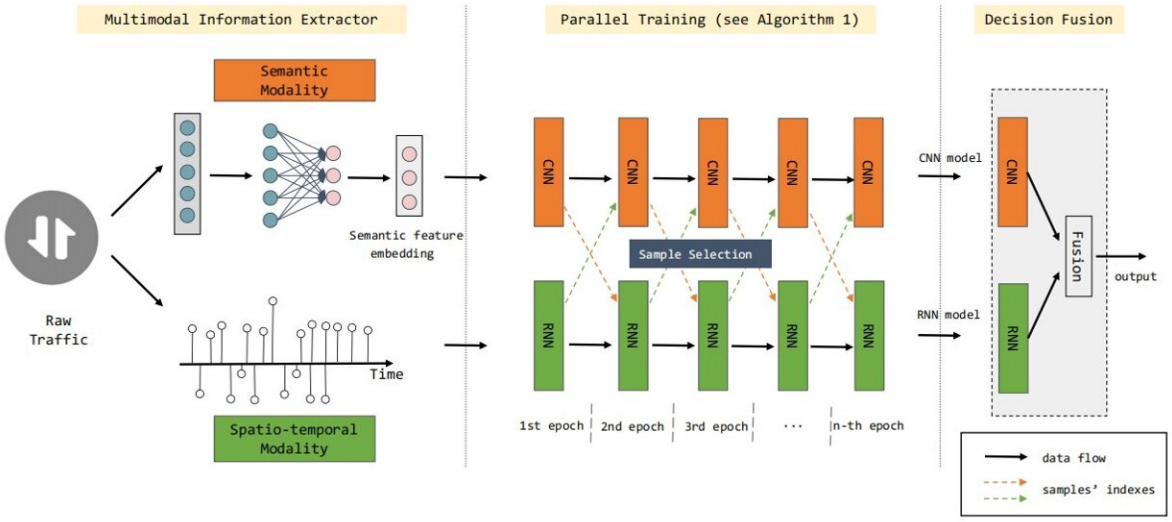
Using multimodal deep learning to detect malicious traffic with noisy labels

February 27 2024



Architecture of MMCo. Credit: Qingjun Yuan, Gaopeng Gou, Yuefei Zhu, Yongjuan Wang

The success of a deep learning-based network intrusion detection systems (NIDS) relies on large-scale, labeled, realistic traffic. However, automated labeling of realistic traffic, such as by sand-box and rule-based approaches, is prone to errors, which in turn affects deep learning-based NIDS.

To solve the problem, a research team led by Yuefei Zhu proposed MMCo, a Co-teaching-like method using multimodal information and

parallel, heterogeneous networks to detect malicious traffic with noisy labels. Unlike existing methods, MMCo is the first LNL method that uses multimodality to maintain disagreement; and the parallel networks in MMCo are heterogeneous and input different modalities of samples, which can mitigate self-control degradation and enhance robustness.

They published their research in *Frontiers of Computer Science*.

In the research, they choose CNN and RNN to learn semantic and spatio-temporal modal information from the traffic. In each mini-batch, CNN and RNN are fed with different modalities of the same subset.

CNN and RNN select for each other the samples they consider more important, i.e., the samples with different distinguish or less loss among all mini-batches. Only these samples will be used for updating the parameters of the networks.

The experimental results show that MMCo can maintain a higher disagreement compared with the existing methods, thus helping the classifiers to learn more correct knowledge, with about 10% higher accuracy.

Future work can focus on investigating the analysis of the representations of two networks in multimodal networks using explainable artificial intelligence, which may help identify and clean malicious traffic with noisy labels.

More information: Qingjun Yuan et al, MMCo: using multimodal deep learning to detect malicious traffic with noisy labels, *Frontiers of Computer Science* (2023). DOI: 10.1007/s11704-023-2386-4

Provided by Higher Education Press

Citation: Using multimodal deep learning to detect malicious traffic with noisy labels (2024, February 27) retrieved 14 May 2024 from https://techxplore.com/news/2024-02-multimodal-deep-malicious-traffic-noisy.html

This document is subject to copyright. Apart from any fair dealing for the purpose of private study or research, no part may be reproduced without the written permission. The content is provided for information purposes only.